# A top-down survey on securing IoT with machine learning: goals, recent advances and challenges

Sania Iqbal* and Shaima Qureshi

Department of Computer Science and Engineering,
National Institute of Technology (Srinagar),
Srinagar, Jammu & Kashmir, India
Email: sania_05phd18@nitsri.ac.in
Email: shaima@nitsri.ac.in
*Corresponding author

**Abstract:** The Internet of Things (IoT) has seen it all from being just another innovation to a leading technology; it is now a binding force that interconnects various aspects of our lives. The IoT's tremendous growth is driven by emerging applications and evolving business models, reinforced by falling cost resources and computing. However, it's heterogeneous nature and restricted existence raise various security concerns for the network operators, IoT service providers, and consumers alike. Machine learning has established itself as an inherent part of several IoT applications and is now taking over to address IoT's critical security challenges. The use of machine learning for securing IoT provides the IoT infrastructure with autonomously updated real-time security features. This paper performs a top-down survey on various active attacks faced by IoT networks and aims to showcase how machine learning has become an integral part of the IoT security model.

**Keywords:** IoT; internet of things; IoT security; IoT security goals; machine learning; machine learning algorithms; deep learning; active attacks; security challenges.

**Reference** to this paper should be made as follows: Iqbal, S. and Qureshi, S. (2022) 'A top-down survey on securing IoT with machine learning: goals, recent advances and challenges', *Int. J. Wireless and Mobile Computing*, Vol. 22, No. 1, pp.38–55.

**Biographical notes:** Sania Iqbal is pursuing her PhD degree from the Department of Computer Science and Engineering, National Institute of Technology (NIT) Srinagar. She has completed her MTech (IT) degree from the Central University of Kashmir in 2018 and BTech (IT) degree from NIT Srinagar in 2015. Her research interests include artificial intelligence, machine learning, deep learning and IoT security.

Shaima Qureshi received her Doctor of Philosophy (PhD) degree from the National Institute of Technology Srinagar. She completed her BE(Hons) Computer Science degree from BITS Pilani, India in 2004 and MS degree in Computer Science from Syracuse University, New York, USA in 2006. She is working as an Assistant Professor in NIT Srinagar since 2008. Her research interests include mobile networks, algorithms, operating systems and machine learning.

## 1 Introduction

The Internet of Things idea dates all the way back to the early 1980s at Carnegie Mellon University, when a vending machine selling soda drinks was linked to the internet to allow for online inventory management. IoT integrates various processes such as identifying, sensing, networking and computation to develop a more intelligent environment that saves time, energy and money. IoT network consists of a set of connected devices ranging from a simple sensor to an elaborate workstation that transfer exchange data to optimise their performance without any human intervention to provide services that offer personalised interaction with the 'things.' The 'thing' can be anything that has the potential to perceive and transmit data over a network. IoT offers a platform for these 'things'– sensors and devices to communicate seamlessly within a smart environment and a convenient means of information sharing across heterogeneous platforms. According to the growth map of IoT charted in Wang et al. (2021) and the projection report (Statista 2021) which predicts more than 30.5 billion devices connected via IoT by 2025, IoT is viewed as a significant source of new data, mostly raw data from different resources collected over the internet. However, for the IoT infrastructure to act intelligently to provide better services with the desired QoS or to improvise its performance, it requires examining data to reveal trends, unseen patterns, hidden correlations and actionable insights. This is where data science comes into action. Data science includes techniques from

various fields, including machine learning and data analysis. It has a prominent role in the widespread use of IoT applications and services by generating meaningful inferences from the massive amount of valuable IoT data to provide better services and applications to its users. Simultaneously, the IoT environment also generates enormous traffic, which can be reviewed using data science to monitor IoT devices intelligently and provide sophisticated security solutions. Thus, when combined with IoT, data science provides better performance to external users and can also strengthen the IoT infrastructure by addressing the core issues like security (Zeadally et al. 2020).

Considering the diverse applications and roles of IoT, this paper primarily focuses on generic IoT networks. The methodology followed in this literature review was to critically investigate the pros and cons of the existing state-of-the-art solutions that aim to address the security aspect of IoT networks. The focus is on security approaches that implement machine learning as the core of the model and addresses any category of active attack identified in this work. Also, since the aim of the review is to comprehend the advances made using machine learning in detecting malicious behaviours in IoT networks, we provide an exhaustive top-down survey of the relevant research works conducted recently over the last few years (specifically 2017–2020 are considered).

In this paper, we list the related surveys in IoT security in general, and then the use of machine learning in IoT security specifically. The next section identifies various IoT security goals, then discusses the challenges faced in implementing the goals, and the subsequent the trade-offs. It is followed by an extensive top-down survey on the use of machine learning to address IoT security issues. The next section focuses on the challenges of implementing machine learning algorithms in IoT environments and suggests solutions.

## 2 Related review works

Till now a plethora of literature has been published on IoT security, its importance, lapses, challenges and possible solutions. However, the relevant literature does not have a holistic approach to securing the IoT network and is either application-specific or focused on designing more generalised intrusion detection systems. An Intrusion Detection System (IDS) is a broad class of systems based on the concept that intruder behaviour varies from normal behaviour and thus is a basic form of defence for a network (Mighan and Kahani, 2021). The architecture of IDS can be host-based or network-based with access to local information and global information, respectively or a hybrid system with the combination of both (Verma and Ranga, 2019a). The domain of IDS is determined by its functionality be it application-specific or general and the performance of any IDS is a combined effect of its architecture and domain. In addition, based on their detection methodologies, IDS can be categorised into anomaly detection, signature or misuse detection and stateful protocol analysis detection.

### *2.1 Review works related to IoT security*

Following is the year-wise distribution of noteworthy reviews and surveys related to IoT security in general, with no specific solution from domain:

Jing et al. (2014) presented the security overview of IoT with respect to its three-layered architecture and traditional wireless networks.

Al-Fuqaha et al. (2015) and Andrea et al. (2015) provided a summary of challenges and emerging solutions for IoT security, Mahmoud et al. (2015) presented the status and solutions pertaining to IoT security challenges. Sadeghi et al. (2015) assessed security scenario of industrial IoT.

Mosenia and Jha (2017) presented a survey on vulnerabilities of edge-side level in IoT architecture and discussed possible measures to address them. Banu et al. (2016) reviewed biologically inspired methods to secure IoT network. Stout and Urias (2016) surveyed the challenges in securing IoT devices and communication.

Lin et al. (2017) and Benzarti et al. (2017) explored security in IoT related networks and possible emerging technologies. Krishna and Gnanasekaran (2017) and Lee and Kim (2017) advocated the need for IoT security at different layers. Yang et al. (2017) and Alaba et al. (2017) presented a security overview in IoT. Mostefa and Abdelkader (2017) surveyed the security aspect of wireless sensor networks as an integrated part of IoT.

Sadique et al. (2018); Kamble and Bhutad (2018) and Sha et al. (2018) addressed open issues and challenges in IoT security. Abdul-Ghani et al. (2018) performed IoT attack survey based on four phased IoT reference attack model. Ammar et al. (2018) surveyed the security architectures of eight IoT frameworks. Stellios et al. (2018) assessed cyberattacks in various IoT-based applications. Kouicem et al. (2018) surveyed proposed IoT security solutions with emphasis on new technologies.

Noor and Hassan (2019) provided IoT security scenario from 2016 to 2018. Zahra and Chishti (2019) assessed the security challenges and issues based on inherent features of IoT and IoT smart infrastructure application domains like city, healthcare, industries, buildings and transport. Neshenko et al. (2019a, 2019b) surveyed security attacks on IoT, its impacts and real-world examples. Gulzar and Abbas (2019); Javeed et al. (2019); Yousuf and Mir (2019); Lu and Xu (2019) and Meneghello et al. (2019) further addressed various perspectives of security in IoT. Hassija et al. (2019) discussed sources of IoT security issues and possible solutions in the light of blockchain, fog computing, edge computing and machine learning.

Podder et al. (2020) and Ande et al. 2020) surveyed IoT security challenges, trends and countermeasures.

Rachit et al. (2021) and Sundaravadivazhagan et al. (2021) reviewed security aspects and threats in IoT. Goyal et al. (2021) surveyed latest developments in IoT security.

Liang and Kim (2021) and Mishra and Pandya (2021) chalked out the evolution of IoT security and its solution.

In addition to above, several works related to intrusion detection systems for IoT are surveyed by Gendreau and Moorman (2016), Zarpelão et al. (2017) and Khraisat and Alazab (2021).

### 2.2 Review works related to machine learning in IoT security

The use of learning-based methods for wireless network security is relatively old and exhausted (Alsheikh et al., 2014), however the literature that focuses on the use of machine learning for securing IoT network is sparse and open ended proposals that discuss possible approaches using various learning algorithms. Cañedo and Skjellum (2016) discussed a fundamental approach to use Artificial Neural Networks (ANN) at the gateway to secure IoT edge nodes. Since last few years the issue of securing IoT network using machine learning approaches have gained some momentum and is being specifically addressed now. Following works review the possible opportunities for deploying machine learning algorithms to secure IoT:

- Al-Garadi et al. (2018); Cui et al. (2018); Xiao et al. (2018a); Moh and Raju (2018); Restuccia et al. (2018) and Xin et al. (2018).
- Liang et al. (2019); Hasan et al. (2019).
- Zeadally and Tsikerdekis (2020); Al-Garadi et al. (2020) and Wu et al. (2020).
- Kuzlu et al. (2021) and Ahmad and Alsmadi (2021).

In addition to above works Buczak and Guven (2016); Da Costa et al. (2019); Chaabouni et al. (2019); Asharf et al. (2020) and Arshad et al. (2020) review IoT network intrusion detection systems based on machine learning algorithms only.

Other related notable works include – Hussain et al. (2020b) and Tahsien et al. (2020) discussed role of machine learning in IoT and enlist learning model-based security solutions for IoT. Koroniotis et al. (2018, 2019) presented a survey on the use of deep learning model to address the issue of botnets only. Uprety and Rawat (2021) surveyed the use of reinforcement learning in IoT security. Few review works address the security concern of a particular IoT application, such as – Liu et al. (2019b) provides a general security overview of smart-critical-IoT infrastructure, Hossain et al. (2019) reviewed the role of big data and machine learning in smart grid security, Alimi et al. (2020) assessed the security of power systems based on machine learning approaches.

From the above discussion it is evident that the surveys related to the deployment of machine learning for securing IoT networks are limited and very few of them have discussed the applied security solutions of practical significance. To our knowledge, this is the first survey of its kind that critically examines the deployment of machine learning in the context of potential threats and attacks for providing security solutions to IoT.

## 3 Identifying goals for protection of an IoT network

IoT is a networking technology and an integration of existing networking technologies, particularly wireless sensor networks, internet and cloud infrastructure. Owing the coexistence and collaboration of such various IoT infrastructure technologies, the security issues get complicated and the possible threats amplified, leaving a vast room for security improvisation. For an IoT infrastructure, the most asset is the data collected. It must be protected from any breach or loss. This protection of IoT data is the main objective of IoT security, and to attain this, we define IoT security goals as:

1) *Security and privacy*: It refers to protecting the IoT node collecting the data, the data collected and stored in any IoT device (Showkat and Qureshi 2020). This goal ensures the three aspects of the CIA security triad: confidentiality, integrity and availability.

   *Confidentiality* is a security principle that controls access to data to ensure only authorised people or devices can access it. Confidentiality of data can be protected by implementing data encryption techniques and access control mechanisms.

   *The integrity* of data refers to the accuracy, consistency and trustworthiness of data over its life cycle. The integrity of data can be ensured by various hashing methods and establishing a baseline for the system. Backups and redundancy plans are also implemented in case of an integrity failure.

   *Availability* of data means that authorised users have guaranteed uninterrupted and timely access to the data. Methods like load balancing; high availability, redundancy, fault tolerance, clustering and RAID are used to achieve availability.

2) *Trust*: Trust is a complex concept. It encompasses different aspects of a system, including its aims, ideas, expectations and potential. In IoT, trust is the enforcement of the established security principles for a system. The trust objectives are usually addressed by deploying a Trust Management framework, which ensures the IoT system's proper and trustworthy functionality. Trust broadly consists of the given objectives:

   a) *Trust between IoT layers*: Proper communication protocols and the transfer of data between the layers of an IoT network are maintained. Modes employed by various IoT layers to interact within and with each other need to ensure data security and privacy for it to be trustworthy.

   b) *Trustworthiness of different IoT nodes*: It addresses the trustworthiness of relationships among IoT components cooperating within a network. Owing the rapid increase in IoT devices, there are multiple sources of trust issues in the IoT environment. Some nodes are reliable, some unreliable and some corrupted as such a stimulus can generate different responses from these nodes. Under such circumstances, the truth has to be inferred from these untrustworthy nodes. Similarly, inconsistency in IoT components regarding addressing or naming, e.g., similar components with different names, needs to be resolved.

3) *Trust between the end-user and the IoT network*: The IoT devices reveal privileged data to the end-user at a particular stage and vice versa. Hence, for the effective deployment of the IoT and its services, the need is to have a degree of trust between the end-user and the IoT network. Also, the user must be trustworthy to have access to the IoT network. His interaction with the system will affect the system's correctness, making it necessary to grade the user's actions.

A collaborative structure containing frameworks for protection, privacy and trust is a reasonable solution for implementing the goals listed above – Security, Privacy and Trust to protect an IoT network. However, given the IoT network's resource and energy constraints, deploying such a collaborative system is a significant challenge.

## 4 Challenges in attaining security goals for an IoT network

IoT has certain features that are the same as wireless sensor networks (Fernandes et al., 2017) yet securing IoT presents a vastly different scenario and a variety of novel challenges. The main challenges being:

1) *Network and device size:* IoT as a network is humungous in size consisting of billions of devices; the devices, on the other hand, are constrained in size, memory, computational power, energy and storage. With energy optimisation as a major criterion in these devices, replacement of batteries being expensive or time-consuming is not an option. Also, the devices are mobile and not always connected to the network. Yugha and Chithra (2020) As such, we must rely on the limited capabilities of the coupled devices to secure this sheer size of the network; this contrasting paradigm of size needs some novel mechanisms to address the security issues without affecting the network performance and at the same time ensuring scalability.

2) *Human component:* Unlike other existing networks, IoT interacts with humans, which is one of its critical and most disruptive aspects (Restuccia et al. 2018). This dynamic and mutual human-machine interaction involved in IoT is beneficial in data sharing and the use of machine learning concepts in IoT. However, the same interaction poses a significant security threat, as the shared information is prone to be stolen or subjected to improper use. Besides the reliability of information generation is also critical, the permission, willingness, and ability to do it.

3) *Heterogeneity:* IoT networks connect a variety of devices, and these IoT devices are connected with various protocols. As the IoT infrastructures grow, the increase in the number and types of connected devices pose the risk of severe damages and latency detection as massive IoT data will be stored in the clouds (Subbarayalu et al., 2019). Such practices will endanger the IoT network as well as the data centre. Thus, the primary security concern with large IoT networks is the built-in heterogeneous types of devices and protocols, which are extremely complex to secure. Since this cannot be satisfactorily achieved by traditional security mechanisms designed for wireless networks or existing IoT networks, the need for a holistic security model catering to IoT's heterogeneity of components is imminent.

4) *Scale of attacks:* With the advent of technology, attacks on IoT networks have also improvised in strength and depth. Also, the enormous growth of the IoT network has impacted its security model. The vast size and growth make the IoT network a profitable platform for fraudulent activities. This also makes the IoT platform a potential resource to launch further large-scale attacks (Arshad et al. 2020). In multi-stage attacks, attacks are carried over multiple stages, each attempting to exploit a specific vulnerability. Similarly, in a multi-attack model, a combination of attacks is launched on the network simultaneously. There is a need to find methods to intelligently detect such attacks in IoT networks in a pre-emptive manner.

5) *IoT botnets:* The main challenges for securing IoT devices are IoT botnets. Botnets are an assembly of compromised devices build by infecting connected devices. IoT botnets take advantage of their collective computing power to spread volumes of malicious data, persistently targeting more and more devices (Angrishi, 2017). In order to mitigate the threat of IoT botnets, security should become a significant factor in IoT development. IoT networks were built with insecure and poor security mechanisms since they were not a priority as companies needed profit or lacked security expertise. Botnet and malware in IoT need to be tackled head on Pokhrel et al. (2021).

## 5 Security issues in IoT and their corresponding ML-based solutions

Despite the growth, IoT devices nowadays face challenges majorly not from lack of computation power, restricted energy, less storage, and bandwidth but due to associated security risks of each device, link and network. Data tampering and network attacks are two diametrically opposite things; data tampering can have multiple sources, network attacks being one of them. However, for an IoT network, the most valuable thing is its data, and thus the primary motive for any attack, especially an active attack, is to tamper or steal its data (Solangi et al., 2018). Significant sources of active IoT network attacks and the existing solution to them using machine learning models are described in the Table 1

**Table 1** Sources of active IoT network attacks and the existing ML-based solutions for such attacks

| *Attacks and its sub-types* | *Description* | *IoT Layer* | *Effect on network* | *ML-based solutions and their performance* |
|---|---|---|---|---|
| *1: Tampering (node capture)* | A node is physically captured to take over its control, thus exposing its critical data and its position in the network. | Physical Layer | –DoS attack against availability<br>–Attack data integrity | • (Chatterjee et al., 2019) RF-PUF: uses a 3-layer ANN for device identification, Accuracy 99%<br>• (Li et al., 2020) Truncated Gradient Detection (TGD) and Online Gradient Descent detection (OGD), Real-time detection rate, improved by 10–20%<br>• (Elngar, 2018) ANN-GA(Genetic Algorithm) tamper detection mechanism, Performance 98.51%<br>• (Das et al., 2018)LSTM classifier authenticates by uniquely identifying low power transmitters. Accuracy: 88.10 % in presence of noise and attenuation<br>• (Sahu et al., 2021) SVM based device fingerprinting. Precision: Single attack : 0.78, multi-attack : 0.70<br>• (Zhu et al., 2021) IoT device monitoring system using decision tree classifier, Accuracy 96.71% |
| *2: Collision attack* | The adversary sends packets to collide with each transmitted packet so that when the corrupt packets are received, they are discarded, retransmitted and eventually dropped. | Data Link Layer | –Increases re-transmission rate | • (Wang et al., 2020) MMV-compressed sensing model for detection with a Matching Pursuit (MP) Multiple response Sparse Bayesian Learning (MSBL) algorithm (MP-MSBL) algorithm reconstructs superimposed signals, Detection Rate >95%<br>• (Lee et al., 2020) CoRL–Collaborative Reinforcement learning-based MAC protocol using stateless Q-learning, Convergence rate > 34 % than conventional Q-learning<br>• (Moy et al., 2020) IoTligent-based solution using UCB reinforcement learning algorithm. PoC success rate of 94%<br>• (Nguyen et al., 2019a) Transfer learning using deep learning models previously trained for computer vision, evaluated over real and synthetic data, Total Accuracy 94% |
| *3: Denial of sleep attack* | Sleep deprivation torture, here a node is prevented from going to sleep to deplete its energy resources. When accomplished by performing a continuous collision attack, it is labelled as an exhaustion attack. | Data Link Layer | –Forces nodes to shut down, attacking availability | • (Kumar et al., 2020) TP2SF (Trustworthy Privacy-Preserving Secured Framework) based on blockchain, machine learning (XGBoost) and fog computing. Efficiency >91%<br>• (Fotohi and Firoozi Bari, 2020) WSN-FAHN implements mobile sink using Hopfield neural network, clustering and AES. PDR > 91%<br>• (Myridakis et al., 2020) SmartShell uses K-means clustering on device current supply characteristic with TPR of 100% using DoS |
| *4: De-synchronisation* | A group of de-synchronised nodes results from the adversary transmitting packets in time slots reserved for authentic users | Data Link Layer<br>Transport Layer | –Increases collision rate in the network<br>–Effects fairness of link | • (Brun et al., 2018) DNN based attack detection model trained on legitimate packet-derived statistical characteristics.<br>• Accurate Attack probability detection |

**Table 1** Sources of active IoT network attacks and the existing ML-based solutions for such attacks (continued)

| *Attacks and its sub-types* | | *Description* | | *IoT Layer* | *Effect on network* | *ML-based solutions and their performance* |
|---|---|---|---|---|---|---|
| *5: Spoofing* | | The hostile node imitates a victim node's address to create multiple legitimate identities and use them anywhere in the network. | | Data Link Layer | –Attacks authentication and access control of devices | • (Xiao et al., 2016) Q-learning and Dyna-Q-based spoofing detection, Average error rate < 5%<br>• (Xiao et al., 2018b) dFW and IAG-based authentication scheme, with both the false alarm rate (FPR) and miss detection rate < 1%.<br>• (Han et al., 2017) DQN-based anti-jamming communication system, Spoofing detection 95%, User identification 92%<br>• (Mohamed Shakeel et al., 2018) LDQN: Learning-based Deep-Q-Network Accuracy 98.79% |
| *6: Channel unfairness attack* | | Intermittent channel blackouts cause channel unfairness due to sporadic use or collision or constant channel access. | | Data Link Layer | –Degrades the QoS of the network<br>–It introduces a delay in the network | • (Wang et al., 2020) MMV-compressed sensing model for detection with an MP-MSBL algorithm reconstructs superimposed signals under the Security Spreading Code Generation (SSCG) framework, Detection rate >95%<br>• (Hussain et al., 2017) Resource Allocation and Congestion control using Q-Learning, Performance depends on learning rate and reward |
| *7: Denial of service (DoS) attacks* | *7a: Jamming* | A malicious device sends a jamming signal by transmitting at the same frequency, contributing to the channel's noise. Jamming can be conducted continuously or temporarily or by targeting only the useful packets. Exploits probability distribution of packet arrival times in DLL against packet transmission. | | Physical Layer<br>Data Link layer | –Decreases the SNR below acceptable levels.<br>–Hampers data transmission | • (Han et al., 2017) DQN-based anti-jamming communication system, accuracy: Spoofing detection 95%, User identification 92%<br>• (Dromard et al., 2017) ORUNADA, an online, real-time and scalable unsupervised network anomaly detector based on the discrete time-sliding window and the incremental grid clustering algorithm IDGCA<br>• SVM classifier (Gurulakshmi and Nesarani, 2018), Traffic: HTTP, TCP and ICMP, Accuracy: ~96%<br>• K-NN classifier (Gurulakshmi and Nesarani, 2018) Traffic: HTTP, TCP, and ICMP, Accuracy: large-featured set: 90%, less-featured set: 98%<br>• (Verma and Ranga, 2019c) Accuracy :RF: 94.94%, CART:91.98% , MLP:82.76% , AB: 90.37%,GBM : 92.98%, XGB: 93.15%, ETC:82.99%<br>• Deep Learning-based Intrusion Detection System (DL-IDS)–implements the Spider Monkey Optimisation (SMO) algorithm with the Stacked-Deep Polynomial Network (SDPN) (Otoum et al., 2020)<br>• (Alabsi et al., 2019) E-ACO based DoS detection followed by RPL-SR for secure transmission |
| | *7b: Flooding* | MAC-Flooding | By sending redundant data to its neighbours, the malicious node takes advantage of medium access fairness. | Data Link Layer | –Deplete energy resources.<br>–Exhaust channel bandwidth resources | |

**Table 1** Sources of active IoT network attacks and the existing ML-based solutions for such attacks (continued)

| *Attacks and its sub-types* | | *Description* | | *IoT Layer* | *Effect on network* | *ML-based solutions and their performance* |
|---|---|---|---|---|---|---|
| | | HELLO-Flooding | An adversary with a long transmission range sends out marketing messages to the entire network in order to persuade other nodes that it is in their neighbourhood and that they should select it as their parent node, routing all messages through it. | Network Layer | –Increases delay and energy consumption<br>–State of confusion is created as the adversary is in the shortest path for each node | • (Kumar et al., 2020)Trustworthy Privacy-Preserving Secured Framework (TP2SF) based on blockchain, machine learning(PCA), and fog computing. Efficiency >91%<br>• (Brun et al., 2018) DNN-based attack detection model trained on legitimate packet-derived statistical characteristics, Attack probability detection 100%<br>• (Amouri et al., 2020) Two-stage cross layer-based IDS, Linear regression for the detection threshold, F1 score varied between 93% and 99.36%<br>• (Thamilarasu and Chawla, 2019)Deep Learning-based Integrated intrusion detection, Precision rate: 96<br>• (Verma and Ranga, 2019b) ELNIDS (Ensemble Learning-based Network Intrusion Detection, System)<br>Accuracy: Boosted Trees: 94.4%; Bagged Trees: 93.3%.<br>Subspace Discriminant: 79%; RUS Boosted Trees:94%<br>• (Churcher et al., 2021)Experimental multiclass analysis,<br>Classifier, Accuracy: KNN – 99%; SVM – 79%; DT – 96%; NB – 94%; RF – 95%; ANN – 97%; LR – 74%<br>• (Huong et al., 2021a) LCHA- Low-Complexity detection solution with High Accuracy based on DNN, Accuracy >98% |
| | | SYN-Flooding | The adversary sends several TCP links requests, never commencing the connection request, causing the victim's half-open connection buffer to be overwhelmed. | Transport Layer | –Exhausts the energy and memory of the nodes | |
| | *7c: Path-based DoS* | An attacker sends fabricated or replayed packets to overwhelm an end to the end communication path. This is done from a long distance so that all nodes along the path are affected. | | Application Layer | –Disables large portions of the network by exhaustion | |
| | *7d: Sensor overwhelming* | Attackers target sensors with spurious interruption or overwhelm them with bogus messages and false signals. | | Application Layer | –Bandwidth Overload<br>–Wastage of node's energy (Gavrić and Simić 2018) | |
| *8: Node-replication attack* | *8a: Clone-ID attack* | Attackers get access to a significant portion of the network by replicating the identity of the compromised node. The attacker might use the exactly similar logical identity of the compromised node on several physical nodes. | | Network Layer | –Introduces inconsistency in the network by sabotaging data and protocols | • (Verma and Ranga, 2019b) ELNIDS (Ensemble Learning-based Network Intrusion Detection System), Accuracy: Boosted Trees – 94.4 %; Bagged Trees – 93.3%, Subspace Discriminant – 79%; RUS Boosted Trees – 94%<br>• (Mbarek et al., 2020) Enhanced NIDs with replica detection protocol for 6LowPAN networks uses 7ayesian analysis, Detection Accuracy 95% |

**Table 1** Sources of active IoT network attacks and the existing ML-based solutions for such attacks (continued)

| *Attacks and its sub-types* | | *Description* | *IoT Layer* | *Effect on network* | *ML-based solutions and their performance* |
|---|---|---|---|---|---|
| *9: Routing attacks* | *9a: Wormhole attack* | Two intruders construct a tunnel and direct all traffic through it, via Packet Replay and Packet Encapsulation | Network Layer | –Effects performance in terms of synchronisation and localisation | • (Raza et al., 2013) SVELTE- an IDS based on the 6Mapper algorithm Accuracy: Sinkhole: 90%; Grey hole: >80% • (Shukla, 2017) ML-IDS to detect wormhole attacks Detection rate: KM-IDS:70–93%; DT-IDS:71–80%; Hybrid IDS:71–75% • (Cervantes et al., 2015) INTI (Intrusion detection for Sinkhole attacks over 6LoWPAN for InterneT of ThIngs) Detection rate: fixed nodes: 92% & mobile nodes:75% • (Jamali and Fotohi, 2017) DAWA using fuzzy logic and an artificial immune system, FPR: 0.01 at 20% malicious node rate • (Ioannou and Vassiliou, 2019) cSVM Anomaly Detector • Accuracy: 100% and 81% on a topology not of training data set • (Amouri et al., 2020) Two-stage cross layer-based IDS, Linear regression for the detection threshold Accuracy: F1 score varied between 93% and 99.36% • (Thamilarasu and Chawla, 2019) Deep Learning-based Integrated intrusion detection. Precision rates: Blackhole attack: 97.2%, Sinkhole attack: 99.5% & Wormhole attack :96% • (Verma and Ranga, 2019b) ELNIDS (Ensemble Learning-based Network Intrusion Detection System) • Accuracy: Boosted Trees – 94.4 %; Bagged Trees – 93.3%. Subspace Discriminant – 79%; RUS Boosted Trees – 94% • (Hussain et al., 2020a) Supervised ML-based data-centric misbehaviour detection model for IoV with plausibility check Precision: SVM – 96.40, K-NN – 88.42, Naïve Bayes – 89.56, Random Forest – 99.17, Ensemble-Boosting – 88.70, Ensemble-Voting – 88.64 • (Verma and Ranga, 2019c) Effectiveness RPL-NIDDS17 dataset developed for RPL on ML-based classifiers, Accuracy: DT – 94.07, LR – 79.79, NB – 80.71, ANN – 93.99, EM – 77.17 • (Deng et al., 2019) Sybil Intrusion prevention system, Fuzzy C means Clustering, Detection rate: 96.8% |
| | *9b: Sinkhole attack* | A sinkhole is a compromised malicious node that attracts the entire traffic by faking an optimal path to its neighbouring nodes. It creates opportunities for follow-on attacks. | | –Targets network topology –Compromises access control | |
| | *9c: Blackhole attack* | The malicious node drops the packets received for forwarding. When a blackhole node is a sinkhole too, all the traffic is halted. | | –Attacks reliability due to increased packet drop | |
| | *9d: Grayhole (Selective Forwarding) attack* | The compromised node drops some packets while modifies others then reliably forwards them. It is a variant of black hole that forwards only control messages. | | –Effects dataflow by the corruption of packet loss rate | |
| | *9e: Sybil attack* | A type of masquerading,the attacker retains multiple logical identities, confusing other nodes to obtain conflicting routing paths that pass through it. | | –Reduces fault-tolerance –Corrupts routing –False data injection | |
| | *9f: Misdirection* | Adversary intentionally forwards messages to wrong paths; neighbours update this misinformation in the routing tables. | | –Effects availability of network | |
| | *9g: Network partitioning* | The otherwise fully connected network is partitioned into smaller networks that cannot communicate despite being connected. | | –Severs the communication link | |
| | *9h: Routing loop* | A loop is introduced in the routing path by spoofing routing updates; as such, messages will be forever forwarded. | | –Depletion of energy resources –Node failure | |
| | *9i:Rushing* | The attacker forwards a high transmission routing packet to a node, which accepts this packet, discards other such packets that reach later and uses it as a valid route. | | –Compromises data confidentiality –Cause DoS in the network | |
| | *9j: Altered routing information* | Exchanged routing information is tampered with or spoofed by malicious nodes to affect routing tables. | | –Invalidates the routing scheme in use | |

**Table 1** Sources of active IoT network attacks and the existing ML-based solutions for such attacks (continued)

| *Attacks and its sub-types* | | *Description* | | *IoT Layer* | *Effect on network* | *ML-based solutions and their performance* |
|---|---|---|---|---|---|---|
| *10: Protocol exploit* | *10a: RPL (Ipv6 Routing Protocol over Low power and Lossy network) Exploit* | Local-Repair Attack | The attacker periodically sends local repair control messages that send the neighbouring nodes into the local repair cycle. | Network Layer | –Negatively impacts the delivery ratio<br>–Increases end to end delay | • (Raza et al., 2013) and (Kalyani and Vydeki, 2018) SVELTE–an IDS based on 6Mapper algorithm using 'Ebbits' approach, detection rate> 90%<br>• (Neerugatti and Mohan Reddy, 2019) MLTKNN, based on K-nearest neighbour algorithm with TPR>90%<br>• (Yavuz et al., 2018) DL-based detection model with model accuracy–Rank Attack: 94.9%, Hello Flood: 99.5%, Version Attack: 99.2%<br>• (Said et al., 2020) OSVM-based rank attack detection, Detection rate > 90%<br>• (Alabsi et al., 2019) Protocol RPL-SR with balanced clustering and secure routing, Delay < 2.5 ms, PDR >40% & Energy Consumed <.025mW<br>• (Verma and Ranga, 2019c) Effectiveness RPL-NIDDS17 dataset developed for RPL on ML-based classifiers,<br>• Classifier and accuracy: DT – 94.07, LR – 79.79, NB – 80.71, ANN – 93.99, EM – 77.17<br>• (Fatima-tuz-Zahra et al., 2020) proposes use of SVM to secure RPL<br>• (Momand et al., 2021) MLRP, Machine Learning-based secure RPL routing protocol, PDR – 76.8%<br>• (Sharma and Verma, 2021) AIELMA – ANN-based Intrusion detection system, Accuracy – 100%<br>• (Kfoury et al., 2019) SOM-IDS<br>• Self-organising map-based intrusion detection<br>• (Anitha and Arockiam, 2019) ANN-IDS<br>• Based on MLP based ANN, Detection rate 100% |
| | | Rank Attack | The attacker increases the DODAG rank value in the hierarchical tree. Thus, it gets many child nodes, thereby attracting massive traffic towards itself. | | –Alters routing scheme<br>–Passive attacks (sniffing and identity attack) or active attacks (blackhole or sinkhole attack) | |
| | | Version Attack | The incremented version number of the DODAG tree is published, causing un-optimised trees with inconsistent loops &rank. | | –Inconsistent and unoptimised network topology | |
| | | DIS (DODAG Information Solicitation) Attack | The receiver receives DIS messages with false IP addresses, regenerates it, forms new DODAG tree. | | –Increases the control overhead<br>–Combined with other attacks | |
| | | Neighbour Attack | The attacker broadcasts the DIO message without sender information, causing the victim node to update its table. | | –Increases end-to-end communication latency<br>–Phoney alterations in network topology | |
| | *10b: 6LoWPAN (Ipv6 over Low-power Wireless Personal Area Network) Exploit* | Fragment Duplication Attack | The node processes without authentication, spurious data placed in the fragmentation chain. | Network Layer | –Renders network prone to DoS<br>–Depletion of resources during reassembly | • (Mbarek et al., 2020)Enhanced NIDs with replica detection protocol for 6LowPAN based networks uses 8ayesian analysis, Accuracy 95%<br>• (Sheikhan and Bostani, 2016) Anomaly-based and Misuse-based intrusion detection for 6LoWPAN networks<br>ML-based misuse detection module-Detection rates: SVM – 95.05%, NB – 81.00%, CART – 97.15 %, MOPF – 96.20%s<br>• (Napiah et al., 2018)CHA-IDS (Compression Header Analyser Intrusion Detection System)<br>ML Classifier accuracies: J48: 99.4444%, LR: 94.1667%, MLP: 96.6667%, NB: 97.2222%, RF: 99.4444%, SVM: 93.333% |
| | | Authentication & Confidentiality Attack | Network does not authenticate new nodes and lacks confidentiality mechanisms too. | | –Attacker can easily gain access to the network<br>–Makes network prone to attacks like spoofing | |
| | | Buffer Reservation Attack | Attacker occupies the limited buffer space reserved for packet reassembly. | | –Packet drop as the reassembly buffer is always full. | |

**Table 1** Sources of active IoT network attacks and the existing ML-based solutions for such attacks (continued)

| *Attacks and its sub-types* | | *Description* | | *IoT Layer* | *Effect on network* | *ML-based solutions and their performance* |
|---|---|---|---|---|---|---|
| | *10c: MQTT exploit* | BEAST (Browser Exploit Against SSL/TLS) | An MITM attack on an encrypted session via adaptive chosen plaintext attack with predictable initialisation vectors. | Transport Layer | –Attacks confidentiality and integrity of communication link<br>–Compromises authenticity of a session | • (Moustafa et al., 2019) AdaBoost ensemble classifier using NB, DT, and ANN with a detection rate of 99% for HTTP and DNS datasets.<br>• (Syed et al., 2020)<br>• AODE classifier: Average accuracy:96.75% & Average MTT:8.70<br>C45 classifier: Average accuracy:96.12% & Average MTT:38.51<br>MLP classifier: Average accuracy:86.30% & Average MTT:1463.43<br>• (Hindy et al., 2020) ML-based IDS for MQTT attacks<br>Classifier, Precision: SVM (Linear Kernel)- 98.66%, SVM (RBF kernel)– 97.02%, NB – 98.37%, RF– 98.97%, LR – 99.44%, KNN – 99.9%, DT-99.95% |
| | | CRIME (Compression Ratio Info-leak Made Easy) | An authenticated web session is hijacked by side-channel attack to discover session tokens. | | –Loss of data integrity and confidentiality<br>–Allows the launch of further attacks | |
| | | RC4 Biases | Invariance Weakness of RC4 cipher is used to launch recovery attacks. | | –Access session data<br>–Attack is optimised using request structure | |
| | | Heartbleed | Exploits OpenSSL's heartbeat functionality, Request is not verified. | | –Network's privileged information is exposed with no trace | |
| *11: Session hijacking* | | It entails using a web session control function, such as a session key, to obtain unauthorised entry to a system's information or services. | | Transport Layer | –Attacks the confidentiality of the session. | • Hybrid NIDS based on the AC (Subbarayalu et al. 2019)<br>Accuracy: 97.17% & False Positives: 0.01%<br>• (Huong et al., 2021b) LCHA- Low-Complexity detection solution with High Accuracy: DNN – 96%, RNN – 96%, CNN – 98%, NN – 98% |
| *12: CoAP exploit* | *12a: Parsing attacks* | A remote node is overburdened by performing an arbitrary code exploiting the processing logic of complex parsers. | | Application Layer | –Introduces vulnerabilities through code discrepancies | • (Kumar and Gandhi, 2020) Enhanced DTLS based CoAP protocol, smart gateway-based authentication, and authorisation<br>Packet loss ratio of 0.45 at time-out of the 60s<br>• (Herrero, 2020) Dynamic CoAP mode selection algorithm using maximum likelihood estimation and linear regression, Average error <= 10%<br>• (Roselin et al., 2019)6LoWPAN-CoAP communication monitoring tool<br>Classifier with Accuracy, ROC : NB: 93.42%, 82.50%; K-Star: 93.95%, 94.70%; KNN: 94.39%, 89.7%; J48: 94.92%, 88%; RF: 93.95%, 93%; RT: 94.06%, 78.1%; SVM: 93.95%, 64.3%<br>• (Granjal et al., 2018) Misbehaviour Detection in CoAP-based networks<br>SVM kernel with multi-class PCA & Accuracy:-<br>linear : 0.212513, rbf : 0.509824, poly: 0.283868, sigmoid: 0.618408<br>SVM kernel with multi-class LDA & Accuracy:-<br>linear : 0.932782, rbf : 0.632368, poly: 0.933816, sigmoid: 0.753361<br>SVM kernel with binary-class LDA & Accuracy:-<br>linear : 0.858325, rbf : 0.830403, poly: 0.810238, sigmoid: 0.927094 |
| | *12b: aching attack* | A proxy with caching capabilities gains access, posing a risk to clients sharing data | | | –Compromises integrity of request-response data | |
| | *12c: Amplification attack* | An adversary uses a CoAP node for amplification, converts a minor attack packet into a bigger packet to overload it. | | | –Nodes get implicated in DoS attack | |
| | *12d: Spoofing attack* | An attacker exploits the lack of handshake in UDP to spoof certain or entire response messages or by spoofing a multicast request for a target node. | | | –Challenges authentication and access control of nodes. | |
| | *12f: Cross-protocol attack* | The attacker exploits the lack of context in UDP-based protocols. It sends a fake source address to a victim, which handles the UDP packet via different protocol. | | | –Circumvents firewall rules that prevent communication between the attacker and target | |
| | *12j: Attack on constrained nodes* | Constrained nodes are prone to tampering, including the recovery of keying data and timing attacks. | | | –Subvert the entire group that share security credentials | |

**Table 1** Sources of active IoT network attacks and the existing ML-based solutions for such attacks (continued)

| *Attacks and its sub-types* | *Description* | *IoT Layer* | *Effect on network* | *ML-based solutions and their performance* |
|---|---|---|---|---|
| *13: False data injection* | Captured nodes intentionally inject false data to influence the overall results or readings, affecting the data at the semantic level. | Application Layer | –Influences overall result to affect the logic | • (Kumar et al., 2020) TP2SF (Trustworthy Privacy-Preserving Secured Framework), Efficiency >91%<br>• (Liu et al., 2019a) Perceptron Detection (PD) and Perceptron Detection with enhancement (PDE) for detecting compromised nodes<br>• (Esmalifalak et al., 2013) Bad Data Detection, SVM : F1 =0.956 |
| *14: Re-programming attack* | Adversaries take advantage of vulnerable times like before re-programming or when patching needs to be done. It sends spurious data to the nodes and transforms them into a compromised or unstable, or unresponsive state. | Application Layer | –Targets the availability and functionality of the nodes<br>–Precursor to other attacks like botnets, DoS, or Man in the Middle | • (Kumar and Lim, 2019) EDIMA (Early Detection of IoT Malware Network Activity) Accuracy: RF – 88.8%, KNN – 94.44%, Gaussian NB – 77.78%<br>• (Nguyen et al., 2019b) DïoT (Federated Self-learning Anomaly Detection System), Distributed DNN model: TPR: 95.6 %, FPR: 0.0%, Speed: 257 ms<br>• (Hafeez et al., 2018) IoT-Keeper, Gateway Keeper- Fuzzy C-Mean clustering and Fuzzy interpolation scheme: Accuracy: 98.2% & FPR: 0.01<br>• (TienChin-Wei et al., 2020) Use of ELF and opcode features for training Accuracy with opcode:- ANN – 97.76%, CNN – 98.37%, SVM – 97.76%<br>• (Thorat et al., 2021) Predictive alarm manager at IoT gateway<br>• Ensemble Method (RF + CB): Avg. Precision: 0.88 & Best precision:0.99 |

## 6 Challenges in using ML for IoT security

Machine learning algorithms were initially designed to process large amounts of data with no resource constraints. Machine learning algorithms were initially deemed unsuitable for IoT networks with limited resources. The combination of cloud computing and IoT enabled data analytics via machine learning. Machine learning is becoming an integral part of IoT infrastructure, particularly in delivering security solutions. To use machine learning in real-time and achieve the above security goals, the following challenges must be overcome:

1 *Resource constraints:* The limited nature of IoT devices is due to their inherent diversity and applications (Zahra and Chishti, 2019). Because IoT devices lack processing power and energy, they cannot run traditional machine learning algorithms. While the ML learning part is compute-intensive, however, running ML-based inferences in parallel on many nodes consumes power and network bandwidth, leaving the IoT infrastructure with limited resources to perform its intended functions. Even as machine learning algorithms' processing requirement is improving, there is always a trade-off between performance and power, where power consumption is the most limiting factor. Using an optimal resource allocation algorithm for security model training and evaluation is the more traditional approach. Using distributed platforms to design and deploy an IoT security model can optimise computing resources, like cloud (Alsharif and Rawat, 2021) and fog (Abeshu and Chilamkurti, 2018). Edge computing provides flexibility and low latency. To avoid the need for feature selection techniques, deep learning models with hyper parameter tuning methods (Mishra and Pandya, 2021) can be used.

2 *Data heterogeneity and privacy:* The IoT data is heterogeneous in syntax and semantics generated from various sources and uses various protocols, making efficient and unified generalisation difficult. Heavy pre-processing is required for data reduction and integration (Saleem and Chisti, 2019). Aside from real-time security, data must be available in a proper format, which can be difficult if data is ambiguous. So that classifiers can train and evaluate efficiently, the data sets must be balanced in terms of attack and non-attack data distribution for classifiers to train and evaluate efficiently. This prevents the learning model from over- or under-generalising the malicious network behaviour. The privacy and security of IoT data varies depending on the application and data source. It must be ensured that user data is secure, especially if it comes from sensitive sources. To avoid contradictions, data availability and features must be consistent across all platforms. This ensures that the modelling is done on a real data set, not a spurious one. Since real-world IoT data sets are rare, they lack balanced data distribution and are marked by privacy constraints.

So, researchers usually use synthetic data sets, which are computationally expensive and do not depict real-world attacks. The authenticity and data distribution of a data set ultimately determine the learned model's authenticity and ability to identify true cases.

3 *Complexity of learning algorithms:* The complexity measures of a machine learning algorithm are defined as the static part, including the feature selection and modification and the type of learning curve, while the dynamic part includes model tuning and deployment. The overall complexity includes algorithm learning, model training, computational, and implementation complexity (Hussain et al., 2020b). This, plus the ongoing training, adds to the complexity and resource exhaustion. They are more complex than traditional machine learning models because they have more parameters. This means that the latter complexity measures do not apply explicitly to deep learning models. The expressive capacity and model effective complexities of deep learning models are defined in terms of model framework, model size, optimisation process, and data complexity (Hu et al., 2021) An ML or DL complexity analysis is a complex procedure designed to provide insight into the model and its data and resource requirements. Pseudo-standard practices to define algorithm complexity are being identified. However, because these models are black boxes, it is impossible to determine the system's functionality in terms of reusability and interpretability. A single machine learning model cannot achieve all identified security goals. Unlike humans, each model is trained to address a specific problem. For diverse malicious activity categories, diverse models and thus data sets are required, and the discussed complexity of learning algorithms hinders such approaches. Envisaging ensemble-based approaches (Verma and Ranga, 2019b) and explainable learning models (Liang et al., 2019) can lead to a possible holistic security approach.

4 *Inherent challenges of ML and DL algorithms:* The machine learning models are application-specific, and the functionality depends on the training data. A large and reliable data set is required for a generalised model free of over-fitting issues. A learned model's reusability is desired for reuse in a similar domain. A relevant data set is required for accurate training, even in transfer learning, where the learned model is applied to a new but related task. A data set from two completely different backgrounds hinders learning (Rosenstein et al., 2005) and can be more costly than starting from scratch. Also, the inherent security of ML and DL techniques is critical; the algorithm should not be vulnerable to certain programming or input attacks. Pitropakis et al. (2019) found that machine learning is vulnerable to several attacks. There have been recent serious attacks on DL: Adversarial Attacks on DL (Akhtar and Mian, 2018), Evasion Attacks (Biggio et al., 2013), Poisoning Attacks (Jagielski et al., 2018), Black Box attack (Papernot et al., 2017) and Backdoor Attack (Salem et al., 2020). These attacks make the model unstable (Barreno et al., 2010) and degrade its performance. For example, using learned models in security compromises the security module and entire infrastructure, effectively rendering the system useless. To effectively deploy the machine learning algorithm as a standalone security model, these vulnerabilities must be discovered and addressed.

5 *Performance requirements:* The performance of predictive models is influenced by the training data as well the hyper-parameters, which determine the learning behaviour. Changing these hyper-parameters can significantly impact predictive performance and resource usage. Similarly, the security model's timeliness is critical. It is therefore necessary to optimise the use of dynamic data and machine learning-based security models. Mohapatra et al. (2020) evaluated different machine learning algorithms for sensor fault detection in real-time, with the Random Forest classifier having the best performance with a classification score of around 88 units. However, deep learning models require more time for predictive analysis, and resource usage increases with complexity (Palvanov and Cho, 2018). Also, machine learning algorithms, convergence times vary. For example, reinforcement learning has a slower convergence time than other methods, affecting the system's responsiveness and dynamic behaviour. Timeliness and latency are key performance indicators for security model. A real-time security model is also required. Its hyper-parameters must be quickly defined and cannot be changed frequently, as certain critical and interdependent IoT networks cannot afford any security downtime (Liao et al., 2017).

6 *Evolution of malicious attacks:* While machine learning-based security model is data-dependent, sources of attack grow rapidly. Malicious code concurrently evolves to bypass security models, and adversaries too evaluate attacks on trained models (Liang et al., 2019). Because these attacks are constantly evolving, the security model must be flexible. Incremental learning models can be implemented using high dimensional training data. To make such modelling computationally possible, online learning paradigm is feasible, as shown in Li et al. (2019) and Dromard et al. (2017).

## 7 Conclusion

The ease of use of IoT in real-world applications exposes it to a wide range of physical and virtual threats. Traditional security solutions cannot address IoT-specific issues such as mobility, heterogeneity, resource constraints, broad coverage and rapid changeability. Instead of just secure communication, IoT requires a security model that can learn, predict network behaviour, and have an intelligent security system. The goal is to create a machine learning-based intelligent IoT security model that works in real-time and has a high detection rate. In this survey, we examined potential active attack threats against

IoT networks, and then evaluated machine learning-based security solutions. A majority of supervised learning-based ML classifiers are used to detect malicious IoT network behaviour. The main advantage of supervised learning is that it can use historical network traffic patterns to train predictive models with small training data sets. Unsupervised learning, reinforcement learning, and deep learning are gaining traction for use in secure IoT networks. However, machine learning and its security approaches still face many obstacles. To address some of these issues, machine learning models and certain computing paradigms such as cloud, fog and edge computing are collaborating. To secure IoT networks, future models will need a more efficient and possibly hybrid machine learning system. The use of smart data for such learning models, data interpretation and visualisation should also be investigated.

## References


Abdul-Ghani, H.A., Konstantas, D. and Mahyoub, M. (2018) 'A comprehensive IoT attacks survey based on a building-blocked reference model', *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 9, No. 3. Doi: 10.14569/IJACSA.2018.090349.

Abeshu, A. and Chilamkurti, N. (2018) 'Deep learning: the frontier for distributed attack detection in fog-to-things computing', *IEEE Communications Magazine*, Vol. 56, No. 2, pp.169–175. Doi: 10.1109/MCOM.2018.1700332.

Ahmad, R. and Alsmadi, I. (2021) 'Machine learning approaches to IoT security: a systematic literature review', *Internet of Things*, Vol. 14. Doi: 10.1016/j.iot.2021.100365.

Akhtar, N. and Mian, A. (2018) 'Threat of adversarial attacks on deep learning in computer vision: a survey', *arXiv:1801.00553 [cs]*.

Alaba, F.A. et al. (2017) 'Internet of things security: a survey', *Journal of Network and Computer Applications*, Vol. 88, pp.10–28. Doi: 10.1016/j.jnca.2017.04.002.

Alabsi, B.A. et al. (2019) 'DDoS attack aware environment with secure clustering and routing based on RPL protocol operation', *IET Circuits, Devices and Systems*, Vol. 13, No. 6, pp.748–755. Doi: 10.1049/iet-cds.2018.5079.

Al-Fuqaha, A. et al. (2015) 'Internet of things: a survey on enabling technologies, protocols, and applications', *IEEE Communications SurveysTutorials*, pp.2347–2376. Doi: 10.1109/COMST.2015.2444095.

Al-Garadi, M.A. et al. (2018) 'A survey of machine and deep learning methods for internet of things (IoT) security', *arXiv:1807.11023 [cs]*

Al-Garadi, M.A. et al. (2020) 'A survey of machine and deep learning methods for internet of things (iot) security', *IEEE Communications Surveys Tutorials*, Vol. 22, No. 3, pp.1646–1685. Doi: 10.1109/COMST.2020.2988293.

Alimi, O.A., Ouahada, K. and Abu-Mahfouz, A.M. (2020) 'A review of machine learning approaches to power system security and stability', *IEEE Access*, Vol. 8, pp.113512–113531. Doi: 10.1109/ACCESS.2020.3003568.

Alsharif, M. and Rawat, D.B. (2021) 'Study of machine learning for cloud assisted IoT security as a service', *Sensors*, Vol. 21, No. 4. Doi: 10.3390/s21041034.

Alsheikh, M.A. et al. (2014) 'Machine learning in wireless sensor networks: algorithms, strategies, and applications', *IEEE Communications Surveys Tutorials*, Vol. 16, No. 4, pp.1996–2018. Doi: 10.1109/COMST.2014.2320099.

Ammar, M., Russello, G. and Crispo, B. (2018) 'Internet of things: a survey on the security of IoT frameworks', *Journal of Information Security and Applications*, Vol. 38, pp.8–27. Doi: 10.1016/j.jisa.2017.11.002.

Amouri, A., Alaparthy, V.T. and Morgera, S.D. (2020) 'A machine learning based intrusion detection system for mobile internet of things', *Sensors*, Vol. 20, No. 2. Doi: 10.3390/s20020461.

Ande, R. et al. (2020) 'Internet of things: evolution and technologies from a security perspective', *Sustainable Cities and Society*, Vol. 54. Doi: 10.1016/j.scs.2019.101728.

Andrea, I., Chrysostomou, C. and Hadjichristofi, G. (2015) 'Internet of things: security vulnerabilities and challenges', *Proceedings of the IEEE Symposium on Computers and Communication (ISCC)*, pp.180–187. Doi: 10.1109/ISCC.2015.7405513.

Angrishi, K. (2017) 'Turning internet of things (IoT) into internet of vulnerabilities (IoV) : IoT botnets', *arXiv:1702.03681 [cs]* [Preprint].

Anitha, A. and Arockiam, L. (2019) 'ANNIDS: artificial neural network based intrusion detection system for internet of things', *International Journal of Innovative Technology and Exploring Engineering*, Vol. 8, No. 11, pp.2583–2588. Doi: 10.35940/ijitee.K1875.0981119.

Arshad, J. et al. (2020) 'A review of performance, energy and privacy of intrusion detection systems for IoT', *Electronics*, Vol. 9, No. 4. Doi: 10.3390/electronics9040629.

Asharf, J. et al. (2020) 'A review of intrusion detection systems using machine and deep learning in internet of things: challenges, solutions and future directions', *Electronics*, Vol. 9, No. 7. Doi: 10.3390/electronics9071177.

Banu, R., Ali Ahammed, G.F. and Fathima, N. (2016) 'A review on biologically inspired approaches to security for internet of things (IoT)', *Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*. pp.1062–1066. Doi: 10.1109/ICEEOT.2016.7754848.

Barreno, M. et al. (2010) 'The security of machine learning', *Machine Learning*, Vol. 81, No. 2, pp.121–148. Doi: 10.1007/s10994-010-5188-5.

Beltrán-García, P. et al. (2019) 'IoT botnets | SpringerLink', *International Congress of Telematics and Computing*, Springer, pp.247–257. Doi: 10.1007/978-3-030-33229-7_21.

Benzarti, S., Triki, B. and Korbaa, O. (2017) 'A survey on attacks in internet of things based networks', *Proceedings of the International Conference on Engineering MIS (ICEMIS)*, pp.1–7. Doi: 10.1109/ICEMIS.2017.8273006.

Biggio, B. et al. (2013) 'Evasion attacks against machine learning at test time', in Blockeel, H. et al. (Eds): *Machine Learning and Knowledge Discovery in Databases*, Springer, Berlin, Heidelberg, pp.387–402. Doi: 10.1007/978-3-642-40994-3_25.

Brun, O. et al. (2018) 'IoT attack detection with deep learning', *ISCIS Security Workshop*.

Buczak, A.L. and Guven, E. (2016) 'A survey of data mining and machine learning methods for cyber security intrusion detection', *IEEE Communications Surveys Tutorials*, Vol. 18, No. 2, pp.1153–1176. Doi: 10.1109/COMST.2015.2494502.

Cañedo, J. and Skjellum, A. (2016) 'Using machine learning to secure IoT systems', *Proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST)*, pp.219–222. Doi: 10.1109/PST.2016.7906930.

Cervantes, C. et al. (2015) 'Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for internet of things', *Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp.606–611. Doi: 10.1109/INM.2015.7140344.

Chaabouni, N. et al. (2019) 'Network intrusion detection for IoT security based on learning techniques', *IEEE Communications Surveys Tutorials*, Vol. 21, No. 3, pp.2671–2701. Doi: 10.1109/COMST.2019.2896380.

Chatterjee, B. et al. (2019) 'RF-PUF: enhancing IoT security through authentication of wireless nodes using in-situ machine learning', *IEEE Internet of Things Journal*, Vol. 6, No. 1, pp.388–398. Doi: 10.1109/JIOT.2018.2849324.

Churcher, A. et al. (2021) 'An experimental analysis of attack classification using machine learning in IoT networks', *Sensors*, Vol. 21, No. 2. Doi: 10.3390/s21020446.

Cui, L. et al. (2018) 'A survey on application of machine learning for internet of things', *International Journal of Machine Learning and Cybernetics*, Vol. 9, No. 8, pp.1399–1417. Doi: 10.1007/s13042-018-0834-5.

Da Costa, K.A.P. et al. (2019) 'Internet of things: a survey on machine learning-based intrusion detection approaches', *Computer Networks*, Vol. 151, pp.147–157. Doi: 10.1016/j.comnet.2019.01.023.

Das, R. et al. (2018) 'A deep learning approach to IoT authentication', *Proceedings of the IEEE International Conference on Communications (ICC)*, pp.1–6. Doi: 10.1109/ICC.2018.8422832.

Deng, L. et al. (2019) 'Mobile network intrusion detection for IoT system based on transfer learning algorithm', *Cluster Computing*, Vol. 22, No. 4, pp.9889–9904.Doi: 10.1007/s10586-018-1847-2.

Dromard, J., Roudière, G. and Owezarski, P. (2017) 'Online and scalable unsupervised network anomaly detection method', *IEEE Transactions on Network and Service Management*, Vol. 14, No. 1, pp.34–47. Doi: 10.1109/TNSM.2016.2627340.

Elngar, A. (2018) 'IoT-based efficient tamper detection mechanism for healthcare application', *International Journal of Network Security*, Vol. 20, No. 3, pp.489–495.

Esmalifalak, M. et al. (2013) 'Detecting stealthy false data injection using machine learning in smart grid', *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, pp.808–813. Doi: 10.1109/GLOCOM.2013.6831172.

Fatima-tuz-Zahra et al. (2020) 'Proposing a hybrid RPL protocol for rank and wormhole attack mitigation using machine learning', *Proceedings of the 2nd International Conference on Computer and Information Sciences (ICCIS)*, pp.1–6. Doi: 10.1109/ICCIS49240.2020.9257607.

Fernandes, E. et al. (2017) 'Internet of things security research: a rehash of old ideas or new intellectual challenges?', *IEEE Security Privacy*, Vol. 15, No. 4, pp.79–84. Doi: 10.1109/MSP.2017.3151346.

Fotohi, R. and Firoozi Bari, S. (2020) 'A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms', *The Journal of Supercomputing*, Vol. 76, No. 9, pp.6860–6886. Doi: 10.1007/s11227-019-03131-x.

Gavrić, Ž. and Simić, D. (2018) 'Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks', *Ingeniería e Investigación*, Vol. 38, No. 1, pp.130–138. Doi: 10.15446/ing.investig.v38n1.65453.

Gendreau, A.A. and Moorman, M. (2016) 'Survey of intrusion detection systems towards an end-to-end secure internet of things', *Proceedings of the IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp.84–90. Doi: 10.1109/FiCloud.2016.20.

Goyal, P. et al. (2021) 'Internet of things: applications, security and privacy: a survey', *Materials Today: Proceedings*, Vol. 34, pp.752–759. Doi: 10.1016/j.matpr.2020.04.737.

Granjal, J., Silva, J.M. and Lourenço, N. (2018) 'Intrusion detection and prevention in COAP wireless sensor networks using anomaly detection', *Sensors*, Vol. 18, No. 8. Doi: 10.3390/s18082445.

Gulzar, M. and Abbas, G. (2019) 'Internet of things security: a survey and taxonomy', *Proceedings of the International Conference on Engineering and Emerging Technologies (ICEET)*, pp.1–6. Doi: 10.1109/CEET1.2019.8711834.

Gurulakshmi, K. and Nesarani, A. (2018) 'Analysis of IoT bots against DDOS attack using machine learning algorithm', *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, pp.1052–1057. Doi: 10.1109/ICOEI.2018.8553896.

Hafeez, I. et al. (2018) 'IoT-KEEPER: securing IoT communications in edge networks', *arXiv:1810.08415 [cs]*

Han, G., Xiao, L. and Poor, H.V. (2017) 'Two-dimensional anti-jamming communication based on deep reinforcement learning', *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, Institute of Electrical and Electronics Engineers Inc., pp.2087–2091. Doi: 10.1109/ICASSP.2017.7952524.

Hasan, M. et al. (2019) 'Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches', *Internet of Things*, Vol. 7. Doi: 10.1016/j.iot.2019.100059.

Hassija, V. et al. (2019) 'A survey on IoT security: application areas, security threats, and solution architectures', *IEEE Access*, Vol. 7, pp.82721–82743. Doi: 10.1109/ACCESS.2019.2924045.

Herrero, R. (2020) 'Supervised classification for dynamic CoAP mode selection in real time wireless IoT networks', *Telecommunication Systems*, Vol. 74, No. 2, pp.145–156. Doi: 10.1007/s11235-019-00646-9.

Hindy, H. et al. (2020) 'Machine learning based IoT intrusion detection system: an MQTT case study', *Proceedings of the 12th International Networking Conference*, pp.73–84.

Hossain, E. et al. (2019) 'Application of big data and machine learning in smart grid, and associated security concerns: a review', *IEEE Access*, Vol. 7, pp.13960–13988. Doi: 10.1109/ACCESS.2019.2894819.

Hu, X. et al. (2021) 'Model complexity of deep learning: a survey', *arXiv:2103.05127 [cs]* [Preprint].

Huong, T.T., Bac, T.P. and Dao Minh, L. et al. (2021a) 'An efficient low complexity edge-cloud framework for security in IoT networks', *Proceedings of the IEEE Eighth International Conference on Communications and Electronics (ICCE)*, pp.533–539. Doi: 10.1109/ICCE48956.2021.9352046.

Huong, T.T., Bac, T.P. and Dao Minh, L. et al. (2021b) 'LocKedge: low-complexity cyberattack detection in IoT edge computing', *IEEE Access*, 9, pp.29696–29710. Doi: 10.1109/ACCESS.2021.3058528.

Hussain, F. and Hassan, S.A. et al. (2020a) 'Machine learning for resource management in cellular and IoT networks: potentials, current solutions, and open challenges', *IEEE Communications Surveys Tutorials*, Vol. 22, No. 2, pp.1251–1275. Doi: 10.1109/COMST.2020.2964534.

Hussain, F. and Hussain, R. et al. (2020b) 'Machine learning in IoT security: current solutions and future challenges', *IEEE Communications Surveys Tutorials*, Vol. 22, No. 3, pp.1686–1721. Doi: 10.1109/COMST.2020.2986444.

Hussain, F. et al. (2017) 'Resource allocation and congestion control in clustered M2M communication using Q-learning', *Transactions on Emerging Telecommunications Technologies*, Vol. 28, No. 4. Doi: 10.1002/ett.3039.

Ioannou, C. and Vassiliou, V. (2019) 'Classifying security attacks in IoT networks using supervised learning', *Proceedings of the 15th International Conference on Distributed Computing in Sensor Systems(DCOSS)*, pp.652–658. Doi: 10.1109/DCOSS.2019.00118.

Jagielski, M. et al. (2018) 'Manipulating machine learning: poisoning attacks and countermeasures for regression learning', *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, IEEE, pp.19–35.

Jamali, S. and Fotohi, R. (2017) 'DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system', *The Journal of Supercomputing*, Vol. 73, No. 12, pp.5173–5196. Doi: 10.1007/s11227-017-2075-x.

Javeed, D. et al. (2019) 'Internet of things (IOT) systems and its security challenges', *International Journal of Advanced Research in Computer Engineering and Technology*, Vol. 8, No. 12, pp.508–512.

Jing, Q. et al. (2014) 'Security of the internet of things: perspectives and challenges', *Wireless Networks*, Vol. 20, No. 8, pp.2481–2501. Doi: 10.1007/s11276-014-0761-7.

Kalyani, S. and Vydeki, D. (2018) 'Survey of rank attack detection algorithms in internet of things', *Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp.2136–2141. Doi: 10.1109/ICACCI.2018.8554702.

Kamble, A. and Bhutad, S. (2018) 'Survey on internet of things (IoT) security issues solutions', *Proceedings of the 2nd International Conference on Inventive Systems and Control (ICISC)*, pp.307–312. Doi: 10.1109/ICISC.2018.8399084.

Kfoury, E. et al. (2019) 'A self-organizing map intrusion detection system for RPL protocol attacks', *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)*, Vol. 11, No. 1.

Khraisat, A. and Alazab, A. (2021) 'A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges', *Cybersecurity*, Vol. 4, No. 1. Doi: 10.1186/s42400-021-00077-7.

Koroniotis, N. et al. (2018) 'Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques | SpringerLink', *Mobile Networks and Management*. *International Conference*, Springer, Cham. Doi: 10.1007/978-3-319-90775-8_3.

Koroniotis, N., Moustafa, N. and Sitnikova, E. (2019) 'Forensics and deep learning mechanisms for botnets in internet of things: a survey of challenges and solutions', *IEEE Access*, Vol. 7, pp.61764–61785. Doi: 10.1109/ACCESS.2019.2916717.

Kouicem, D.E., Bouabdallah, A. and Lakhlef, H. (2018) 'Internet of things security: a top-down survey', *Computer Networks*, Vol. 141, pp.199–221. Doi: 10.1016/j.comnet.2018.03.012.

Krishna, B.V.S. and Gnanasekaran, T. (2017) 'A systematic study of security issues in internet-of-things (IoT)', *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp.107–111.

Kumar, A. and Lim, T.J. (2019) 'EDIMA: early detection of IoT malware network activity using machine learning techniques', *Proceedings of the IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp.289–294. Doi: 10.1109/WF-IoT.2019.8767194.

Kumar, P., Gupta, G.P. and Tripathi, R. (2020) 'TP2SF: a trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning', *Journal of Systems Architecture*. Doi: 10.1016/j.sysarc.2020.101954.

Kumar, P.M. and Gandhi, U.D. (2020) 'Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application', *The Journal of Supercomputing*, Vol. 76, No. 6, pp.3963–3983. Doi: 10.1007/s11227-017-2169-5.

Kuzlu, M., Fair, C. and Guler, O. (2021) 'Role of artificial intelligence in the internet of things (IoT) cybersecurity', *Discover Internet of Things*, Vol. 1, No. 1. Doi: 10.1007/s43926-020-00001-4.

Lee, T., Jo, O. and Shin, K. (2020) 'CoRL: collaborative reinforcement learning-based MAC protocol for IoT networks', *Electronics*, Vol. 9, No. 1. Doi: 10.3390/electronics9010143.

Li, B. et al. (2020) 'A detection mechanism on malicious nodes in IoT', *Computer Communications*, Vol. 151, pp.51–59. Doi: 10.1016/j.comcom.2019.12.037.

Li, J. et al. (2019) 'AI-based two-stage intrusion detection for software defined IoT networks', *IEEE Internet of Things Journal*, Vol. 6, No. 2, pp.2093–2102. Doi: 10.1109/JIOT.2018.2883344.

Liang, F. et al. (2019) 'Machine learning for security and the internet of things: the good, the bad, and the ugly', *IEEE Access*, Vol. 7. Doi: 10.1109/ACCESS.2019.2948912.

Liang, X. and Kim, Y. (2021) 'A survey on security attacks and solutions in the IoT network', *Proceedings of the IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, pp.0853–0859. Doi: 10.1109/CCWC51732.2021.9376174.

Liao, W. et al. (2017) 'Cascading failure attacks in the power system: a stochastic game perspective', *IEEE Internet of Things Journal*, Vol. 4, No. 6, pp.2247–2259. Doi: 10.1109/JIOT.2017.2761353.

Lin, J. et al. (2017) 'A survey on internet of things: architecture, enabling technologies, security and privacy, and applications', *IEEE Internet of Things Journal*, Vol. 4, No. 5, pp.1125–1142. Doi: 10.1109/JIOT.2017.2683200.

Liu, L., Ma, Z. and Meng, W. (2019a) 'Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks', *Future Generation Computer Systems*, Vol. 101, pp.865–879. Doi: 10.1016/j.future.2019.07.021.

Liu, X. et al. (2019b) 'Secure internet of things (IoT)-based smart-world critical infrastructures: survey, case study and research opportunities', *IEEE Access*, Vol. 7, pp.79523–79544. Doi: 10.1109/ACCESS.2019.2920763.

Lu, Y. and Xu, L.D. (2019) 'Internet of things (IoT) cybersecurity research: a review of current research topics', *IEEE Internet of Things Journal*, Vol. 6, No. 2, pp.2103–2115. Doi: 10.1109/JIOT.2018.2869847.

Mahmoud, R. et al. (2015) 'Internet of things (IoT) security: current status, challenges and prospective measures', *Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp.336–341. Doi: 10.1109/ICITST.2015.7412116.

Mbarek, B., Ge, M. and Pitner, T. (2020) 'Enhanced network intrusion detection system protocol for internet of things', in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, Association for Computing Machinery, New York, NY, USA, pp.1156–1163. Doi: 10.1145/3341105.3373867.

Meneghello, F. et al. (2019) 'IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices', *IEEE Internet of Things Journal*, Vol. 6, No. 5, pp.8182–8201. Doi: 10.1109/JIOT.2019.2935189.

Mighan, S.N. and Kahani, M. (2021) 'A novel scalable intrusion detection system based on deep learning', *International Journal of Information Security*, Vol. 20, No. 3, pp.387–403. Doi: 10.1007/s10207-020-00508-5.

Mishra, N. and Pandya, S. (2021) 'Internet of things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review', *IEEE Access*, Vol. 9, pp.59353–59377. Doi: 10.1109/ACCESS.2021.3073408.

Moh, M. and Raju, R. (2018) 'Machine learning techniques for security of internet of things (IoT) and fog computing systems', *Proceedings of the International Conference on High Performance Computing Simulation (HPCS)*, pp.709–715. Doi: 10.1109/HPCS.2018.00116.

Mohamed Shakeel, P. et al. (2018) 'Maintaining security and privacy in health care system using learning based deep-Q-networks', *Journal of Medical Systems*, Vol. 42, No. 10. Doi: 10.1007/s10916-018-1045-z.

Mohapatra, D., Subudhi, B. and Daniel, R. (2020) 'Real-time sensor fault detection in Tokamak using different machine learning algorithms', *Fusion Engineering and Design*, Vol. 151. Doi: 10.1016/j.fusengdes.2019.111401.

Momand, M.D., Khan Mohsin, M. and Ihsanulhaq (2021) 'Machine learning-based multiple attack detection in RPL over IoT', *Proceedings of the International Conference on Computer Communication and Informatics (ICCCI)*, pp.1–8. Doi: 10.1109/ICCCI50826.2021.9402388.

Mosenia, A. and Jha, N.K. (2017) 'A comprehensive study of security of internet-of-things', *IEEE Transactions on Emerging Topics in Computing*, Vol. 5, No. 4, pp.586–602. Doi: 10.1109/TETC.2016.2606384.

Mostefa, B. and Abdelkader, G. (2017) 'A survey of wireless sensor network security in the context of internet of things', *Proceedings of the 4th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, pp.1–8. Doi: 10.1109/ICT-DM.2017.8275691.

Moustafa, N. (2019) *The Bot-IoT Dataset*, IEEE. Available online at: https://ieee-dataport.org/documents/bot-iot-dataset

Moustafa, N., Turnbull, B. and Choo, K.R. (2019) 'An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things', *IEEE Internet of Things Journal*, Vol. 6, No. 3, pp.4815–4830. Doi: 10.1109/JIOT.2018.2871719.

Moy, C. et al. (2020) 'Decentralized spectrum learning for radio collision mitigation in ultra-dense IoT networks: LoRaWAN case study and experiments', *Annals of Telecommunications*, Vol. 75, No. 11, pp.711–727. Doi: 10.1007/s12243-020-00795-y.

Myridakis, D. et al. (2020) 'Enhancing scurity on IoT devices via machine learning on conditional power dissipation', *Electronics*, Vol. 9, No. 11. Doi: 10.3390/electronics9111799.

Napiah, M.N. et al. (2018) 'Compression header analyzer intrusion detection system (CHA – IDS) for 6LoWPAN communication protocol', *IEEE Access*, Vol. 6, pp.16623–16638. Doi: 10.1109/ACCESS.2018.2798626.

Neerugatti, V. and Mohan Reddy, A.R. (2019) *Machine Learning Based Technique for Detection of Rank Attack in RPL based Internet of Things Networks*. Rochester, NY

Neshenko, N. et al. (2019a) 'Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations', *IEEE Communications Surveys Tutorials*, Vol. 21, No. 3, pp.2702–2733. Doi: 10.1109/COMST.2019.2910750.

Nguyen, H.N. et al. (2019b) 'Towards adversarial and unintentional collisions detection using deep learning', *Proceedings of the ACM Workshop on Wireless Security and Machine Learning*, New York, NY, USA, pp.22–24. Doi: 10.1145/3324921.3328784.

Nguyen, T.D. et al. (2019c) 'DÏoT: a federated self-learning anomaly detection system for IoT', *Proceedings of the IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pp.756–767. Doi: 10.1109/ICDCS.2019.00080.

Noor, M.B.M. and Hassan, W.H. (2019) 'Current research on internet of things (IoT) security: a survey', *Computer Networks*, Vol. 148, pp.283–294. Doi: 10.1016/j.comnet.2018.11.025.

Otoum, Y., Liu, D. and Nayak, A. (2019) 'DL-IDS: a deep learning-based intrusion detection framework for securing IoT', *Transactions on Emerging Telecommunications Technologies*, n/a(n/a). Doi: 10.1002/ett.3803.

Palvanov, A. and Cho, Y.I. (2018) 'Comparisons of deep learning algorithms for MNIST in real-time environment', *International Journal of Fuzzy Logic and Intelligent Systems*, Vol. 18(2, pp.126–134. Doi: 10.5391/IJFIS.2018.18.2.126.

Papernot, N. et al. (2017) 'Practical black-box attacks against machine learning', *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, Association for Computing Machinery, New York, NY, USA, pp.506–519. Doi: 10.1145/3052973.3053009.

Pitropakis, N. et al. (2019) 'A taxonomy and survey of attacks against machine learning', *Computer Science Review*, Vol. 34. Doi: 10.1016/j.cosrev.2019.100199.

Podder, P. et al. (2020) 'Review on the security threats of internet of things', *International Journal of Computer Applications*, Vol. 176, No. 41, pp.37–45. Doi: 10.5120/ijca2020920548.

Pokhrel, S., Abbas, R. and Aryal, B. (2021) 'IoT security: botnet detection in IoT using machine learning', *arXiv:2104.02231 [cs]*.

Rachit, Bhatt, S. and Ragiri, P.R. (2021) 'Security trends in Internet of Things: a survey', *SN Applied Sciences*, Vol. 3, No. 1, pp.1–15. Doi: 10.1007/s42452-021-04156-9.

Raza, S., Wallgren, L. and Voigt, T. (2013) 'SVELTE: real-time intrusion detection in the internet of things', *Ad Hoc Networks*, Vol. 11, No. 8, pp.2661–2674. Doi: 10.1016/j.adhoc.2013.04.014.

Restuccia, F., D'Oro, S. and Melodia, T. (2018) 'Securing the internet of things in the age of machine learning and software-defined networking', *IEEE Internet of Things Journal*, Vol. 5, No. 6, pp.4829–4842. Doi: 10.1109/JIOT.2018.2846040.

Roselin, A.G. et al. (2019a) 'Exploiting the remote server access support of CoAP protocol', *IEEE Internet of Things Journal*, Vol. 6, No. 6, pp.9338–9349. Doi: 10.1109/JIOT.2019.2942085.

Rosenstein, M.T. et al. (2005) 'To transfer or not to transfer', *Inductive Transfer: 10 Years Later. NIPS'05 Workshop.*

Sadeghi, A-R., Wachsmann, C. and Waidner, M. (2015) 'Security and privacy challenges in industrial internet of things', *Proceedings of the 52nd Annual Design Automation Conference*, New York, pp.1–6. Doi: 10.1145/2744769.2747942.

Sadique, K.M., Rahmani, R. and Johannesson, P. (2018) 'Towards security on internet of things: applications and challenges in technology', *Procedia Computer Science*, Vol. 141, pp.199–206. Doi: 10.1016/j.procs.2018.10.168.

Sahu, K. et al. (2021) 'Leveraging timing side-channel information and machine learning for IoT security', *Proceedings of the IEEE International Conference on Consumer Electronics (ICCE)*, pp.1–6. Doi: 10.1109/ICCE50685.2021.9427585.

Said, A.M. et al. (2020) 'Machine learning based rank attack detection for smart hospital infrastructure', in Jmaiel, M. et al. (Eds): *The Impact of Digital Technologies on Public Health in Developed and Developing Countries*, Springer International Publishing, Cham. Doi: 10.1007/978-3-030-51517-1_3.

Saleem, T.J. and Chishti, M.A. (2019) 'Data analytics in the internet of things: a survey', *Scalable Computing: Practice and Experience*, Vol. 20, No. 4, pp.607–630. Doi: 10.12694/scpe.v20i4.1562.

Salem, A. et al. (2020) 'Dynamic backdoor attacks against machine learning models', *arXiv:2003.03675 [cs, stat]*

Sha, K. et al. (2018) 'On security challenges and open issues in internet of things', *Future Generation Computer Systems*, Vol. 83, pp.326–337. Doi: 10.1016/j.future.2018.01.059.

Sharma, S. and Verma, V.K. (2021) 'AIEMLA: artificial intelligence enabled machine learning approach for routing attacks on internet of things', *The Journal of Supercomputing*. Doi: 10.1007/s11227-021-03833-1.

Sheikhan, M. and Bostani, H. (2016) 'A hybrid intrusion detection architecture for Internet of things', *Proceedings of the 8th International Symposium on Telecommunications (IST)*, IEEE, Tehran, Iran, pp.601–606. Doi: 10.1109/ISTEL.2016.7881893.

Shelby, Z., Hartke, K. and Bormann, C. (2014) 'The constrained application protocol (CoAP)', *Internet Engineering Task Force (IETF)*.

Showkat, S. and Qureshi, S. (2020) 'Securing the internet of things using blockchain', *Proceedings of the 10th International Conference on Cloud Computing, Data Science Engineering (Confluence)*, pp.540–545. Doi: 10.1109/Confluence47617.2020.9058258.

Shukla, P. (2017) 'ML-IDS: a machine learning approach to detect wormhole attacks in internet of things', *Proceedings of the Intelligent Systems Conference (IntelliSys)*, pp.234–240. Doi: 10.1109/IntelliSys.2017.8324298.

Solangi, Z.A. et al. (2018) 'The future of data privacy and security concerns in internet of things', *Proceedings of the IEEE International Conference on Innovative Research and Development(ICIRD)*, pp.1–4. Doi: 10.1109/ICIRD.2018.8376320.

Statista, L. (2021) *Global IoT and non-IoT connections 2010–2025*, *Statista*. Available online at: www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ (accessed on 20 December 21).

Stellios, I. et al. (2018) 'A survey of IoT-enabled cyberattacks: assessing attack paths to critical infrastructures and services', *IEEE Communications Surveys Tutorials*, Vol. 20, No. 4, pp.3453–3495. Doi: 10.1109/COMST.2018.2855563.

Stout, W.M.S. and Urias, V.E. (2016) 'Challenges to securing the internet of things', *Proceedings of the IEEE International Carnahan Conference on Security Technology (ICCST)*, pp.1–8. Doi: 10.1109/CCST.2016.7815675.

Subbarayalu, V., Surendiran, B. and Kumar, P.A.R. (2019) 'Hybrid network intrusion detection system for smart environments based on internet of things', *The Computer Journal*, Vol. 62, No. 12, pp.1822–1839. Doi: 10.1093/comjnl/bxz082.

Sundaravadivazhagan, D.B., Subashini, D.B. and M, M.M.A. (2021) 'A review on internet of things (IoT): security challenges, issues and the countermeasures approaches', *Psychology and Education Journal*, Vol. 58, No. 2, pp.6544–6560. Doi: 10.17762/pae.v58i2.3188.

Syed, N.F. et al. (2020) 'Denial of service attack detection through machine learning for the IoT', *Journal of Information and Telecommunication*, pp.482–503. Doi: 10.1080/24751839.2020.1767484.

Tahsien, S.M., Karimipour, H. and Spachos, P. (2020) 'Machine learning based solutions for security of internet of things (IoT): a survey', *Journal of Network and Computer Applications*, Vol. 161. Doi: 10.1016/j.jnca.2020.102630.

Thakkar, A. and Lohiya, R. (2020) 'A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges | SpringerLink', *Archives of Computational Methods in Engineering*, Vol. 28, pp.3211–3243. Doi: 10.1007/s11831-020-09496-0.

Thamilarasu, G. and Chawla, S. (2019) 'Towards deep-learning-driven intrusion detection for the internet of things', *Sensors*, Vol. 19, No. 9. Doi: 10.3390/s19091977.

Thorat, P. et al. (2021) 'SDN-based predictive alarm manager for security attacks detection at the IoT gateways', *Proceedings of the IEEE 18th Annual Consumer Communications Networking Conference (CCNC)*. Doi: 10.1109/CCNC49032.2021.9369623.

TienChin-Wei et al. (2020) 'Machine learning framework to analyze IoT malware using ELF and opcode features', *Digital Threats: Research and Practice* [Preprint]. Doi: 10.1145/3378448.

Uprety, A. and Rawat, D.B. (2021) 'Reinforcement learning for IoT security: a comprehensive survey', *IEEE Internet of Things Journal*, Vol. 811, Doi: 10.1109/JIOT.2020.3040957.

Verma, A and Ranga, V. (2019c) 'Machine learning based intrusion detection systems for IoT applications | SpringerLink', *Wireless Personal Communications*, Vol., pp.2287–2310. Doi: 10.1007/s11277-019-06986-8.

Verma, A. and Ranga, V. (2019a) 'ELNIDS: ensemble learning based network intrusion detection system for RPL based internet of things', *Proceedings of the 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, pp.1–6. Doi: 10.1109/IoT-SIU.2019.8777504.

Verma, A. and Ranga, V. (2019b) 'Evaluation of network intrusion detection systems for RPL based 6LoWPAN networks in IoT', *Wireless Personal Communications*, Vol. 108, No. 3, pp.1571–1594. Doi: 10.1007/s11277-019-06485-w.

Wang, J. et al. (2021) 'The evolution of the internet of things (IoT) over the past 20 years', *Computers and Industrial Engineering*, Vol. 155. Doi: 10.1016/j.cie.2021.107174.

Wang, N. et al. (2020) 'Compressed-sensing-based pilot contamination attack detection for NOMA-IoT communications', *IEEE Internet of Things Journal*, Vol. 7, No. 8, pp.7764–7772. Doi: 10.1109/JIOT.2020.2991956.

Wu, H. et al. (2020) 'Research on artificial intelligence enhancing internet of things security: a survey', *IEEE Access*, Vol. 8, pp.153826–153848. Doi: 10.1109/ACCESS.2020.3018170.

Xiao, L. et al. (2016) 'PHY-layer spoofing detection with reinforcement learning in wireless networks', *IEEE Transactions on Vehicular Technology*, Vol. 65, No. 12, pp.10037–10047. Doi: 10.1109/TVT.2016.2524258.

Xiao, L. et al. (2018a) 'IoT security techniques based on machine learning: how do IoT devices use AI to enhance security?', *IEEE Signal Processing Magazine*, Vol. 35, No. 5, pp.41–49. Doi: 10.1109/MSP.2018.2825478.

Xiao, L., Wan, X. and Han, Z. (2018b) 'PHY-layer authentication with multiple landmarks with reduced overhead', *IEEE Transactions on Wireless Communications*, Vol. 17(3), pp.1676–1687. Doi: 10.1109/TWC.2017.2784431.

Xin, Y. et al. (2018) 'Machine learning and deep learning methods for cybersecurity', *IEEE Access*, Vol. 6, pp.35365–35381. Doi: 10.1109/ACCESS.2018.2836950.

Yang, Y. et al. (2017) 'A survey on security and privacy issues in internet-of-things', *IEEE Internet of Things Journal*, Vol. 4, No. 5, pp.1250–1258. Doi: 10.1109/JIOT.2017.2694844.

Yavuz, F.Y., Ünal, D. and Gül, E. (2018) 'Deep learning for detection of routing attacks in the internet of things', *International Journal of Computational Intelligence Systems*, Vol. 12, No. 1, pp.39–58. Doi: 10.2991/ijcis.2018.25905181.

Yousuf, O. and Mir, R.N. (2019) 'A survey on the internet of things security: state-of-art, architecture, issues and countermeasures', *Information and Computer Security*. Doi: 10.1108/ICS-07-2018-0084.

Yugha, R. and Chithra, S. (2020) 'A survey on technologies and security protocols: reference for future generation IoT', *Journal of Network and Computer Applications*, Vol. 169. Doi: 10.1016/j.jnca.2020.102763.

Zahra, S.R. and Chishti, M.A. (2019) 'Assessing the services, security threats, challenges and solutions in the internet of things', *Scalable Computing: Practice and Experience*, Vol. 20, No. 3, pp.457–484. Doi: 10.12694/scpe.v20i3.1544.

Zarpelão, B.B. et al. (2017) 'A survey of intrusion detection in internet of things', *Journal of Network and Computer Applications*, Vol. 84, pp.25–37. Doi: 10.1016/j.jnca.2017.02.009.

Zeadally, S. and Tsikerdekis, M. (2020) 'Securing internet of things (IoT) with machine learning', *International Journal of Communication Systems*, Vol. 33, No. 1. Doi: 10.1002/dac.4169.

Zeadally, S. et al. (2020) 'Harnessing artificial intelligence capabilities to improve cybersecurity', *IEEE Access*, Vol. 8, pp.23817–23837. Doi: 10.1109/ACCESS.2020.2968045.

Zhu, B. et al. (2021) 'IoT equipment monitoring system based on C5.0 decision tree and time-series analysis', *IEEE Access*, pp.1–1. Doi: 10.1109/ACCESS.2021.3054044.